- Disclosing the information to its own affiliates, who may, in turn disclose the information only to the extent that the financial institution can do so; and
- Disclosing the information to any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which it received the information. For example, an institution that received a customer list from another financial institution could disclose the list (1) in accordance with the privacy policy of the financial institution that provided the list, (2) subject to any opt out election or revocation by the consumers on the list, and (3) in accordance with appropriate exceptions under sections 14 and 15.

Other Matters

Fair Credit Reporting Act

The regulations do not modify, limit, or supersede the operation of the Fair Credit Reporting Act.

State Law

The regulations do not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that it is inconsistent with the regulations. A state statute, regulation, order, etc. is consistent with the regulations if the protection it affords any consumer is greater than the protection provided under the regulations, as determined by the FTC.

Grandfathered Service Contracts

Contracts that a financial institution has entered into, on or before July 1, 2000, with a nonaffiliated third party to perform services for the financial institution or functions on its behalf, as described in section 13, will satisfy the confidentiality requirements of section 13(a)(1)(ii) until July 1, 2002, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information.

Guidelines Regarding Protecting Customer Information

The regulations require a financial institution to disclose its policies and practices for protecting the confidentiality, security, and integrity of nonpublic personal information about consumers (whether or not they are customers). The disclosure need not describe these policies and practices in detail, but instead may describe in general terms who is authorized to have access to the information and whether the institution has security practices and procedures in place to ensure the confidentiality of the information in accordance with the institution's policies.[3]

The four federal bank and thrift regulators have published guidelines, pursuant to section 501(b) of the Gramm-Leach-Bliley Act, that address steps a financial institution should take in order to protect customer information. The guidelines relate only to information about customers, rather than all consumers. Compliance examiners should consider the findings of a 501(b) inspection during the compliance examination of a financial institution for purposes of evaluating the accuracy of the institution's disclosure regarding data security.

Examination Objectives

1. To assess the quality of a financial institution's compliance management policies and procedures for implementing the privacy regulation, specifically ensuring consistency between what the financial institution tells consumers in its notices about its policies and practices and what it actually does.
2. To determine the reliance that can be placed on a financial institution's internal controls and procedures for monitoring the institution's compliance with the privacy regulation.
3. To determine a financial institution's compliance with the privacy regulation, specifically in meeting the following requirements:
   - Providing to customers notices of its privacy policies and practices that are timely, accurate, clear and conspicuous, and delivered so that each customer can reasonably be expected to receive actual notice;
   - Disclosing nonpublic personal information to nonaffiliated third parties, other than under an exception, after first meeting the applicable requirements for giving consumers notice and the right to opt out;
   - Appropriately honoring consumer opt out directions;
   - Lawfully using or disclosing nonpublic personal information received from a nonaffiliated financial institution; and
   - Disclosing account numbers only according to the limits in the regulations.
4. To initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

Examination Procedures

A. Through discussions with management and review of available information, identify the institution's information sharing practices (and changes to those practices) with affiliates and nonaffiliated third parties; how it treats nonpublic personal information; and how it administers opt-outs. Consider the following as appropriate:

3 Certain functionally-regulated subsidiaries, such as brokers, dealers, and investment advisers will be subject to privacy regulations issued by the Securities and Exchange Commission. Insurance entities may be subject to privacy regulations issued by their respective state insurance authorities.